THE CAPABILITY OF GOVERNMENT IN PROVIDING PROTECTION AGAINST ONLINE FRAUD: ARE CLASSICAL LIBERALS GUILTY OF THE NIRVANA FALLACY?

Edward Stringham, Ph.D.[*]

ABSTRACT

Online merchants are exposed to serious threats of fraud, which has the potential to cripple electronic commerce. Classical liberals such as Epstein and North believe that markets require prohibitions against fraud and that government can solve the problem. Although the classical-liberal solution seems clear, how it will be implemented is less clear. For government to prohibit online fraud a number of conditions must be met. By compiling evidence from government testimonies and interviews in Silicon Valley, this article studies the extent to which government can provide protections against online fraud. It finds a number of obstacles that inhibit government from enforcing laws against online fraud. Technology moves at a rapid pace and government often lacks the capability to identify those who commit fraud. In addition, questions remain about how domestic law enforcement can enforce laws against fraud around the globe. Even if domestic law enforcement had the ability to identify fraudsters, it would need to rely on law enforcement agencies from around the globe to help enforce the laws. Under these conditions the ability for government to prohibit fraud is extremely limited. Classical liberals appear to be guilty of the Nirvana Fallacy.

1. INTRODUCTION

Electronic commerce poses many potential dilemmas for consumers and businesses alike. In non-face-to-face transactions, consumers need to rely on merchants delivering the product and merchants need to rely on consumers delivering the payment. Although much attention has been paid

---

[*] Department of Economics, San Jose State University. Email: Edward.Stringham@sjsu.edu. The author thanks Peter Boettke, Dan Klein, Peter Leeson, Benjamin Powell, and participants at the Critical Infrastructure Project at George Mason University and at the Association of Private Enterprise Education meetings for helpful comments and suggestions. Research funding from the working group on Law, Economics and Technology of Private Enforcement on the Internet is greatly appreciated. The usual disclaimer applies.

to traditional consumer fraud,[1] merchants are perhaps in an even more difficult situation. Customers at least have the ability to look into the reputation of sellers,[2] whereas merchants have no such luxury. Merchants can check that a bank account has funds, but the order still might be placed with a stolen bank account.[3] Fraud often goes undetected until the cardholder notices his bill, well after the goods have shipped. When a transaction goes sour, the merchant usually has to foot the bill.[4] Even though commerce gives businesses access to many additional customers, it also exposes them to many perpetrators of fraud. In today's world, up to 40 percent of online international orders that merchants receive (but do not necessarily accept) are fraudulent, which has the potential to cripple electronic commerce.[5] If merchants have no recourse when fraud occurs and cannot easily distinguish between good and bad orders, they will end up acting cautiously and turning down a number of legitimate orders. Some merchants may even eschew electronic commerce altogether, and the market will not reach its full potential.

The problem of fraud is real, but what is the solution? Most lawyers and economists are influenced by classical liberal theory and look to government to step in. After all, prohibition against fraud is one of the core functions of government. For example, Microsoft General Counsel Bradford Smith stated, "So long as people use the Internet to perpetrate frauds, steal property, and defame and assault one another, governments will be justified in seeking to prevent such behavior through law."[6] The only people who would deny government such a role are anarchist libertarians who reject government altogether. Chicago Law Professor Richard Epstein provides a representative summary of the limited-government or classical-liberal view: "Under its classical liberal formulation, the great social contract sacrifices liberty, but only to the extent that it is necessary to gain security against force and fraud. Perhaps we might go further, but surely we

---

[1] Karen Alboukrek, *Adapting to a New World of E-Commerce: The Need for Uniform Consumer Protection in the International Electronic Marketplace*, 35 Geo. WASH. INT'L L. REV. 425 (2003); Miriam R. Albert, *E-Buyer Beware: Why Online Auction Fraud Should be Regulated*, 39 Am. BUS. L.J. 575 (2002).

[2] Boettke and Steckbeck document how online merchants can build up their reputation, which can be conveyed with review websites or rating systems such as on eBay. Peter Boettke & Mark Steckbeck, *Akerlof Problems and Hayek Solutions: Local Knowledge and Self-governance in E-Commerce*, *in* AUSTRIAN PERSPECTIVES ON THE NEW ECONOMY (Jack Birner ed., 2003), in press.

[3] Other ways consumers commit fraud against merchants is by disputing a bill, denying they made a transaction or by saying the goods arrived damaged.

[4] Cliff Ennico, Get Yourself Paid: Try these two techniques for dealing with deadbeat customers, Entreprenuer.com, July 07, 2003, http://www.entrepreneur.com/article/0,4621,309711,00.html.

[5] Jeff King, Seminar on Accepting International Orders in Real Time, (Cybersource, Inc.) (File author downloaded 2004).

[6] Bradford L. Smith, *The Third Industrial Revolution: Policymaking for the Internet*, 3 COLUM. SCI. & TECH. L. REV. 1 (2002).

go this far."[7] To Epstein, the government must perform certain roles such as providing law against fraud; otherwise, markets would be unable to function. In contrast to the anarchist libertarians, Epstein argues that one would be a "naïve visionary" to "believe that markets could operate of their own volition without any kind of support from the state."[8] He writes, "It is at this juncture that the rule of law becomes critical to offer a secure framework for these voluntary transactions to take place."[9] Similarly, Nobel Laureate Douglas North states that "realizing the economic potential of the gains from trade in a high technology world of enormous specialization and division of labor characterized by impersonal exchange is extremely rare, because one does not necessarily have repeated dealings, nor know the other party, nor deal with a small number of other people."[10] He concludes, "A coercive third party is essential."[11]

The idea that government is needed to enforce laws against fraud is held not only by classical liberals, but also by the vast majority of lawyers and economists as well.[12] Yet the idea is more of an assumption in economic and legal analysis, rather than a hypothesis which is subjected to investigation. The vast majority of lawyers and economists simply assume that government should prohibit fraud and do not give the issue another thought. Although the classical-liberal solution seems clear, how it will be implemented is less clear. Just because something is *de jure* illegal does not mean that an action is effectively prohibited. Passing a law pronouncing something illegal is easy but effective prohibition requires more than just official proclamations. Princeton economist Avinash Dixit states, "the problem is that [conventional economic theory] takes the existence of a

---

[7] Richard A. Epstein, *Hayekian Socialism*, 58 MD. L. REV. 271 (1999).

[8] *Id.* at 285.

[9] *Id.*

[10] DOUGLAS C. NORTH, INSTITUTIONS, INSTITUTIONAL CHANGE AND ECONOMIC PERFORMANCE 12 (1990).

[11] *Id.* at 35.

[12] Avinash Dixit writes, "Even the most libertarian economists, who deny the government any useful role in most aspects of the economy, allow that making and enforcing laws that give clear definitions of property rights, and ensuring adherence to voluntary private contracts, are legitimate and indeed essential functions of government." AVINASH DIXIT, LAWLESSNESS AND ECONOMICS 2 (2004). Similarly, South Carolina Law Professor Henry Mather maintains that even the most "extreme libertarian theories" still give government the "nightwatchman's task of protecting individual liberty against force and fraud" (332). Henry Mather, *Natural Law and Liberalism*, 52 S.C. L. REV. 331 (2001).

well-functioning institution of state law for granted."[13] In many cases, real world difficulties may make enforcing laws against fraud more difficult than economists and lawyers assume.

Pointing out the problem of fraud is simple but the real question is whether government is capable of solving the problem. One can believe that government has the ability to solve the problem, but that does not mean that the belief is true. In this sense, lawyers and economists might be falling into the trap of what Harold Demsetz called the Nirvana fallacy.[14] Many theorists highlight a problem in the world and then conclude that government can solve it.[15] But rather than jumping to the conclusion that the government has the ability to solve the problem, we must look to see if it really does.

Online merchants sold over $100 billion worth of goods in 2003,[16] and although numerous federal, state, and local agencies have computer divisions that aim to "stop perpetrators of fraud and deception,"[17] the extent to which the law actually helps merchants is unestablished.[18] Since it was passed in 1984, the Computer Fraud and Abuse Act (18 U.S.C. § 1030) has been criticized for being "overly vague and too narrow in scope,"[19] and "largely symbolic."[20] As late as 1996 there were only 174 convictions for computer fraud, which includes hacking, copyright infringement, and gambling fraud. The US Department of Justice writes, "experts have long admitted that there are no centralized computer crime statistics, not even within the law enforcement community."[21] We have to investigate, but we might have a case where the laws are on the books but are not really being enforced.

For the government to be able to stop online fraud, a number of conditions must be met. Former Attorney General Janet Reno highlighted some of the problems in a 2000 "five-year strategy" to develop enforcement ca-

---

13 DIXIT, *supra* note 13, at 3.

14 Harold Demsetz, *Information and Efficiency: Another Viewpoint*, 12 J.L. & ECON. 1 (1969).

15 An example of this is John Rothchild, *Protecting the Digital Consumer: The Limits of Cyberspace Utopianism*, 74 IND. L.J. 893 (1999).

16 Keith Regan, Report: Online Sales Top $100 Billion, E-Commerce Times, June 16, 2004.

17 Mozelle Thompson, *The Challenges of Law in Cyberspace—Fostering the Growth and Safety of E-Commerce Commissioner*, 6 B.U. J. SCI. & TECH. L. 1, (2000) Par. 9.

18 FTC Commissioner Mozelle Thompson stated, "it's not the "Wild, Wild West" out there. Fraud and deception for example in consumer protection, it does not matter whether it occurs on the telephone or on the Internet, it is still illegal." Mozelle W. Thompson, *The Federal Trade Commission and Regulating E-Commerce*, 16 ST. JOHN'S J. LEGAL COMMENT. 609 (2002).

19 Reid Skibell, Cybercrimes *& Misdemeanors: A Reevaluation of the Computer Fraud and Abuse*, 18 BERKELEY TECH. L.J. 909, 912 (2003).

20 Brent Wible, *A Site Where Hackers Are Welcome*, 112 YALE L.J. 1577, 1581 (2003).

21 National White Collar Crime Center and Federal Bureau of Investigations, Internet Fraud Complaint Center 2002 Internet Fraud Report (National White Collar Crime Center) (2003), 16.

pability against cybercrimes.[22] The plan noted that effective enforcement against cybercrime includes the following four requirements:[23]

I) A round-the-clock network of federal, state, and local law enforcement officials with expertise in, and responsibility for, investigating and prosecuting cybercrime;
II) Computer forensic capabilities, which are so essential in computer crime investigations;
III) Adequate legal tools to locate, identify, and prosecute cybercriminals, and procedural tools to allow state authorities to more easily gather evidence located outside their jurisdictions;
IV) Effective partnerships with other nations to encourage them to enact laws that adequately address cybercrime and to provide assistance in cybercrime investigations.[24]

Other requirements exist, but these four requirements touch on some of the most important issues for law enforcement today.[25] Law enforcement requires financial resources, trained personnel, advanced equipment, an understanding of technology, and a capability to identify and track down those who commit fraud. In addition, law enforcement needs legal authority and the ability to enforce those laws. If the government is deficient in any of these ways, its ability to enforce laws against fraud will be diminished. If the probability of capture were to approach zero, government would need to respond by increasing penalties infinitely high to maintain deterrence. Although in theory this would make the law just as effective, whether the government could actually do this has yet to be determined.[26]

This article looks into the extent to which governments have the capability to prohibit online fraud. The focus is fraud against merchants, but much of the analysis might apply to traditional consumer fraud or other types of computer crimes. The article goes through the four requirements outlined by Reno and documents whether government appears likely to be

---

22 Janet Reno, Statement of Janet Reno Attorney General of the United State Before the United States Senate Committee on Appropriations, Subcommittee on Commerce, Justice, and State, "Cybercrime" February 16, 2000.

23 The plan contained ten points but this article focuses on four of the more important ones.

24 Janet Reno, Statement of Janet Reno Attorney General of the United State Before the United States Senate Committee on Appropriations, Subcommittee on Commerce, Justice, and State, "Cybercrime" February 16, 2000.

25 Thomas Kubic of the FBI comes up with a near identical list: "The Internet presents new and significant investigatory challenges for law enforcement at all levels . . . . These challenges include: the need to track down sophisticated users who commit unlawful acts on the Internet while hiding their identities; the need for close coordination among law enforcement agencies; and the need for trained and well-equipped personnel to gather evidence, investigate, and prosecute these cases." Thomas T. Kubic, Statement for the Record, House Committee on the Judiciary, Subcommittee on Crime, June 12, 2001.

26 Wible, *supra* note 21, at 1622.

able to solve the problem of online fraud. Most of what I have learned in the research comes from interviews and conversations with technology workers in Silicon Valley. In this sense, the paper will shed little light on the situation to those who work in the industry. Instead, analysis of the industry may shed light on the extent to which classical-liberal theories apply to markets. Much of the evidence in this paper comes from interviews, which are admittedly anecdotal and have the potential to be biased. Whenever possible, I attempt to supplement information from interviews with quotes from government testimonies or other printed publications. The government testimonies may also be biased, but the direction will unlikely portray them as less capable than they truly are. The readers will be left to interpret whether they think the conditions under which government can prohibit online fraud are met.

Although different interpretations of the evidence may be possible, in my opinion the situation is quite clear. Many obstacles make enforcing laws against online fraud very difficult, if not impossible. Although government does enforce prohibitions in a select few transactions, in the vast majority of transactions, government does not appear to provide any redress, leaving merchants virtually helpless against online fraud. I find that the government is not able to solve the problem as the classical liberals would assume. Interestingly, the market does not break down as classical liberal theory would predict. It appears that classical liberals have a number of incorrect assumptions about markets. Perhaps the theories of Epstein and North are just theories with little applicability to the way the economy works.

2. DOES GOVERNMENT HAVE THE CAPABILITY OF PREVENTING ONLINE FRAUD?

Requirement I: A round-the-clock network of federal, state, and local law enforcement officials with expertise in, and responsibility for, investigating and prosecuting cybercrime.

If government is to enforce laws against fraud, it needs resources, computers, and enough personnel who are up to date in the latest technology. This condition seems as if it should be straightforward, but real-world practicalities get in the way. Despite some economic models that assume law enforcement to be costless,[27] law enforcement agencies have limited budgets and must decide where to allocate their scarce resources. The more government devotes to an endeavor such as online fraud, the less it can de-

---

[27] Karen Clay, *Trade, Institutions, and Credit*, 34 EXPLORATIONS IN ECONOMIC HISTORY, 503 (1997).

vote to other areas of law. Numerous cases of online fraud exist, and to expect government to deal with a significant portion of them may be unrealistic.[28] Bruce Townsend of the U.S. Secret Service stated, "Law enforcement does not have the financial or technological resources to cope with all these cases."[29] Although the U.S. government has been devoting more resources to online fraud in recent years, for much of the history of the Internet, a night watchman was not present.[30] Hiring around-the-clock law enforcement agents devoted to computer crime may be costly, but is at least possible.

Expecting law enforcement to have enough expertise in the latest technologies, on the other hand, is more problematic. Markets and technology are evolving at such a rapid rate that keeping up with all of the latest technologies is extremely difficult. Many agencies do have a number of extremely knowledgeable agents. That does not mean, however, that the agencies can keep up with all occurrences of fraud. With millions of potential incidents of fraud, any individual agent can only do so much. Government would need to hire numerous agents who are up to date with technology, and this may not be possible. One of the main obstacles is labor costs, because government must compete with the private sector for talent. If talented security experts can make more money in the private sector, the government may have a difficult time retaining enough workers who are knowledgeable about the technology.[31] If agencies do not have enough people with a sufficient understanding of the technology, they will be unable to enforce the laws against fraud.

Evidence of this problem was explained by one corporate executive whose company was a victim of a considerable online fraud. Not only were

---

28 Consider the possible objectives for law enforcement. A public interest view would model them preventing crime and a public choice view would model them as taking actions to maximize budget or advance other government interests. Whatever we assume about their goals, they still might not devote resources to preventing online fraud. Agencies understandably might devote resources to where they get the most bang for the buck. If solving computer fraud does not bring the headlines or advance government interests as much as another endeavor, they might not devote as much resources as would be needed.

29 Quoted in Jon Swartz, *Is the Future of E-mail under Cyberattack?*, USA TODAY, June 14, 2004.

30 Rustad writes, "Most states have computer crime statutes, but do not have significant law enforcement presence in cyberspace." Michael Rustad, *Private Enforcement of Cybercrime on the Electronic Frontier*, 11 S. CAL. INTERDISC. L.J. 63, (2001) 98-99. See also CLIFFORD STOLL, THE CUCKOO'S EGG: TRACKING A SPY THROUGH THE MAZE OF COMPUTER ESPIONAGE (1989). Stoll discovered someone stealing time on his computer system and spent months tracking the hacker. After making numerous phone calls to various authorities, he was basically told that they were uninterested because his organization had not sustained losses over $1 million. In the end government became involved because Stoll gave them evidence that the hacker was also breaking into military systems.

31 Rustad writes "Local law enforcement lacks the resources to recruit, train, and retain law enforcement officers with good computer skills. Low salaries and a high turnover of experts in cybercrime curtail the effectiveness of law enforcement at both the state and federal level." Rustad, *supra* note 31, at 99.

the legal authorities unknowledgeable of cutting-edge technologies; they were unknowledgeable about even the simplest technology. The company's own investigation had determined that a man named Mr. Yagolnitser was defrauding the company of money. After the company did the difficult work of identifying the culprit and reporting him to the authorities, was law enforcement any help? The executive said:

> The positive place where [government] failed was in providing security. The natural thinking was that when people are defrauding you, you can go to the police. Maybe Mr. Yagolnitser is not going to go to the police, but maybe we can go to the police and report Mr. Yagolnitser. We proceeded to do that. The FBI showed up at his home and concluded he was totally innocent. We'd given them Web pages. They were asking us, 'What's a banner ad?' [32]

For government to investigate whether someone is guilty of fraud, it needs to be up on current technology. The unawareness of basic aspects of the technology seems to indicate that it was years behind. In an interview, another employee from a Silicon Valley security firm told me, "In my view, government is ten years behind what's going on."[33]

One possible solution would be to devote more resources to government law enforcement,[34] but how much this would solve the problem is uncertain. One has to consider how much government would need to know to enforce all the laws. Whereas private companies spend significant resources mastering technologies that they know they will use, government would have to spend significant resources mastering all technologies that people may or may not use. To be able investigate any particular case, government would need a working knowledge of the systems employed by each company. Does government have this capability? Michael Vatis, Director of the FBI's National Infrastructure Protection Center, was quite frank that the answer is no. Vatis said, "It would be impossible for us to retain experts in every possible operating system or network configuration."[35] Given the limited resources of government and the numerous technologies in existence, law enforcement agencies are understandably unable to keep track of all of them. Under these circumstances, wrongdoers have the ability to move their efforts to technologies with which governments are

---

32 Presentation, Independent Institute, San Francisco, CA. April 21, 2004.

33 Personal interview, San Jose, CA. June 30, 2004.

34 Most government agencies believe that the solution lies with more money. For example, Janet Reno stated, "Resource issues are also critical. We must ensure that law enforcement has an adequate number of prosecutors and agents . . . trained in the necessary skills and properly equipped to effectively fight cybercrime." Statement of Janet Reno Attorney General of the United State Before the United States Senate Committee on Appropriations, Subcommittee on Commerce, Justice, and State, "Cybercrime" February 16, 2000.

35 Michael Vatis, Statement of Michael A. Vatis on Cybercrime Before the Senate Judiciary Committee, Criminal Justice Oversight Subcommittee and House Judiciary Committee, Crime Subcommittee, February 29, 2000.

less familiar.[36] Without a knowledge of the various systems, government agencies may be unable to investigate.

One can dream up a world where government knows all technologies inside out and where government knows as much about the future course of technology as private companies. This may be possible, but there is little evidence that this is likely. In countries that rely on such a model, the track record of government guiding technology has not been positive. Government agencies appear to be at least one step behind everyone else.[37] Without enough people with an understanding of the latest technology, government will be unable to enforce laws against fraud.[38] This brings into question whether government is capable of enforcing laws that classical liberals say government needs to enforce.

Requirement II: Computer forensic capabilities, which are so essential in computer crime investigations.

Despite the poor track record of law enforcement agencies in recent years, one can imagine a world in which they are able to keep up with technological change. Even if this were the case, government still may be unable to enforce laws against online fraud. The next requirement for effective law enforcement is the ability to locate and identify those who commit fraud. But difficulties collecting evidence make enforcement of laws against online fraud quite difficult. The first reason investigating fraud can

---

[36] The problem of shifting activities to avoid prohibitions also surfaces with the law as well. Rustad describes what he calls a Cyberlaw Enforcement Lag: "By the time a statute is enacted to counter an Internet-related threat, the creative cybercriminal finds new technologies to bypass an essential element of the prohibited act or offense." Rustad, *supra* note 31, at 96.

[37] Brent Wible, *A Site Where Hackers Are Welcome*, 112 YALE L.J. 1577, 1581 (2003) ("Enforcement remains difficult, especially given the near impossibility of prosecuting attempts under 18 U.S.C. 1030(b), and the need for a great investment of time, resources, and skill—even assuming that local law enforcement agents have the requisite training.").

[38] Karen Alboukrek, *Adapting to a New World of E-Commerce: The Need for Uniform Consumer Protection in the International Electronic Marketplace*, 35 GEO. WASH. INT'L L. REV. 425, 440 (2003) ("Until law enforcement catches up with computer technology, [market participants] will be virtually unprotected from crime in the electronic marketplace.").

[39] Rustad, *supra* note 31, at 98 (2001) ("Internet crimes are seldom detected or prosecuted largely because there is no traditional crime scene.").

be difficult is the high degree of anonymity in non-face-to-face transactions. Although some types of fraud involve shipping goods to an actual address, other types of fraud involve no physical goods, so the fraudster need not ever reveal his real address. Where traditional law enforcement entailed sending investigators to the scene of the crime, online fraud has far fewer clues.[39]

With no witnesses to interview and no footprints to follow, law enforcement may simply be unable to figure out who is committing the fraud. A Report of the President's Working Group on Unlawful Conduct on the Internet (hereinafter President's Working Group) explains, "Another thorny issue stems from the lack of identification mechanisms on global networks . . . . Simply stated, given the current state of technology, it can be difficult to accurately identify an individual."[40] Even if they know that a law has been broken they may not know who the lawbreaker is. The government may be unable to identify the perpetrator or may not even know where to begin looking. A digital trail, if one even exists, can span around the globe.[41] As the President's Working Group explains:

> The communication may also pass through carriers in a number of different countries, each in different time zones and subject to different legal systems. Indeed, each of these complications may exist within a single transmission. This phenomenon makes it more difficult (and sometimes impossible) to track criminals who are technologically savvy enough to hide their location and identity.[42]

With each communication, the fraudster can use a different path, so figuring out the location and identity of the fraudster is often impossible.

Matters become even more problematic when fraudsters take active steps to hide their identity.[43] People can forge identities, forge IP addresses, use stolen accounts, and employ anonymity tools that make identification less likely.[44] Janet Reno admits, "Criminals can use a variety of methods to hide their tracks, allowing them to operate anonymously or through masked

---

[40] President's Working Group on Unlawful Conduct on the Internet, The Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet, March 2000.

[41] "The communications of a hacker or other criminal may pass through as many as a dozen (or more) different types of carriers, each with different technologies (e.g., local telephone companies, long-distance carriers, Internet service providers ("ISPs"), and wireless and satellite networks)." *Id.*

[42] President's Working Group, *supra* note 40.

[43] Wible, *supra* note 37, at 1581.

[44] "Sophisticated criminals can alter data concerning the source and destination of their communications, or they may use the Internet account of another." *Frontier*, *supra* note 40.

[45] Janet Reno, Statement of Janet Reno Attorney General of the United State Before the United States Senate Committee on Appropriations, Subcommittee on Commerce, Justice, and State, "Cybercrime" February 16, 2000.

identities. This makes it difficult—and sometimes impossible—to hold the perpetrator criminally accountable."[45] The President's Working Group writes, "Encryption now presents and will continue to present a challenge to law enforcement confronting Internet-related crime. Robust encryption products make it difficult or impossible for law enforcement to collect usable evidence using traditional methods."[46] All of this "can plainly frustrate legitimate law enforcement efforts."[47] Matters become even more difficult if fraudsters are also hackers and have the ability to modify data that could be used as evidence.[48] Even if the data existed at one point in time, if the information can be deleted or altered, it can confuse an investigation.[49]

Computer forensic capabilities are also complicated by the fact that computer data are often not stored. Internet providers and networks have numerous users, and unless they track and report all user activities to law enforcement agencies, the activities of a fraudster may not be traced. Reno stated:

> Even if criminals do not hide identities online, we still might be unable to find them. The design of the Internet and practices relating to retention of information means that it is often difficult to obtain traffic data critical to an investigation. Without information showing which computer was logged onto a network at a particular point in time, the opportunity to determine who was responsible may be lost.[50]

Some communications may be recorded but not saved for any length of time, while other communications may go unrecorded.[51] If government lacks the necessary evidence to investigate a fraud, the fraud will go unsolved.

These technical difficulties pose obstacles for identifying perpetrators of online fraud. Although accessing, recovering, and decrypting data necessary for an investigation may be technically feasible, expecting that government will have the resources to do it in more than just a few cases may be unrealistic. In a few high-profile cases, the government has indeed caught perpetrators of online fraud, but the vast majority of cases go unre-

---

46 President's Working Group, *supra* note 40.

47 *Id.*

48 Albert writes, "Because of the ephemeral nature of information on the Internet, online fraud cases differ from traditional fraud cases, as data can be purged or reworked in such a way as to hinder investigation into suspected Internet fraud." Albert, *supra* note 1, at 592.

49 President's Working Group on Unlawful Conduct on the Internet, The Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet, March 2000, p.23.

50 Janet Reno, Statement of Janet Reno Attorney General of the United State Before the United States Senate Committee on Appropriations, Subcommittee on Commerce, Justice, and State, "Cybercrime" February 16, 2000.

51 President's Working Group, *supra* note 40, at 30, 32.

ported, uninvestigated, or unsolved.[52] Without being able to identify the perpetrators of online fraud, the de facto situation is that government is unable to enforce the laws. Douglas North argues that anarchic markets can function when trading is face to face, but argues that markets cannot function when trading is relatively anonymous.[53] Perhaps one should apply his logic to law enforcement. As markets become more anonymous, how will government have the capability of enforcing the law?[54]

Requirement III: Adequate legal tools to locate, identify, and prosecute cybercriminals, and procedural tools to allow state authorities to more easily gather evidence located outside their jurisdictions.

Even if government could keep up with technology and locate and identify fraudsters, government still may lack the legal authority to enforce laws against fraud. Because online fraud can be committed from anywhere on the globe, a number of jurisdictional issues arise. The lack of geographical boundaries on the Internet gives companies access to many potential customers,[55] but it also exposes them to many potential fraudsters.[56] A

---

52 Alex Kim, et al., *Fraud Over the Internet: The Same Old Story, Different Medium*, LEGAL COLUMN ARCHIVES (Ford Marrin, Esposito, Witmeyer & Gleser, LLP, New York, NY), Jan. 1999, http://www.fmew.com/archive/fraud; *see also* Wible, *supra* note 20, at 1577.

53 NORTH, *supra* note 10, 34-35.

54 Santa Clara Law Professor David Friedman predicts that government will become less able to enforce the law over time in his unpublished book manuscript Future Imperfect. David Friedman, Future Imperfect (Feb. 10, 2003) (unpublished manuscript), http://patrifriedman.com/prose-others/fi/commented/Future_Imperfect.html.

55 Karen Alboukrek, *Adapting to a New World of E-Commerce: The Need for Uniform Consumer Protection in the International Electronic Marketplace*, 35 Geo. Wash. Int'l L. Rev. 425, 429 (2003).

56 Reno states, "The Internet is a global medium that does not recognize physical and jurisdictional boundaries. A hacker—armed with no more than a computer and modem—can access computers anywhere around the globe. They need no passports and pass no checkpoints as they commit their crimes." *Cybercrime: Hearing Before the Subcomm. on Commerce, Justice, and State of the S. Committee on Appropriations,* 106th Cong. (2000) (Statement of Janet Reno, Attorney General of the United States).

57 The President's Working Group writes, "In short, cybercriminals are no longer hampered by the existence of national or international boundaries, because information and property can be easily transmitted through communications and data networks. As a result, a criminal no longer needs to be at the actual scene of the crime (or within 1,000 miles, for that matter) to prey on his or her victims." President's Working Group, *supra* note 40.

fraudster might reside in one country, use computers in a second country, and commit fraud against a company in a third country.[57] What laws apply? And what law enforcement agency has jurisdiction in such a case? The fact that fraud takes place across geographical boundaries poses a number of problems.

The first problem stems from the fact that laws and legal procedures between countries differ. For example, if one government outlaws an action but another does not, the first government may be unable to apply the laws to the citizens of the second country.[58] Similar problems arise if one government treats fraud as a criminal matter and another treats it as a civil matter. The United States government has signed a number of extradition treaties with other countries, but unless both countries criminalize the act, the U.S. may be unable to pursue a case originating in the other country.[59] The President's Working Group recognizes, "When one country's laws criminalize high-tech and computer-related crime and other country's laws do not, cooperation to solve a crime, as well as the possibility of extraditing the criminal to stand trial, may not be possible."[60] Laws often differ greatly between countries and even differ within the same country through time; for example, the Computer Fraud and Abuse Act was adopted in 1984 and was amended in 1986, 1994, and 1996.[61] Even if a country adopted the exact same laws as those in the United States, unless they continue updating them over time, the two sets of laws might become incompatible.

When a case involves residents from other nations, a number of problems surface. Can law enforcement in the first country issue subpoenas, interview witnesses, and seize equipment for residents in the second nation if the action is not prohibited in that nation?[62] Each country has different ways of dealing with suspects, so how countries should deal with suspects

---

[58] David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367 (1996).

[59] The President's Working Group wrote, "The issue of dual criminality is not an academic or theoretical matter. In 1992, for example, hackers from Switzerland attacked the San Diego Supercomputer Center. The U.S. sought help from the Swiss, but the investigation was stymied due to lack of dual criminality (i.e., the two nations did not have similar laws banning the conduct), which in turn impeded official cooperation. Before long, the hacking stopped, the trail went cold, and the case had to be closed." President's Working Group, *supra* note 40.

[60] *Id.*

[61] *Id.*

[62] *Id.*

[63] Rustad, *supra* note 31, at 94.

in other countries is unsettled.[63] The President's Working Group highlights the difficulties associated with international investigations.[64] Consider what happens when a U.S. law enforcement agency has a search warrant from U.S. courts. Law enforcement may be authorized to search computers within the U.S., but does the warrant enable it to search computers in other countries? Even if a search has been authorized by the US government, another country may not consider the search legitimate. Problems arise with computer investigations because the location of computers is often unknown. Do governments have the authority to search computers around the globe just because a government says they can? The President's Working Group states: "ignorance of physical location may not excuse a trans-border search; consider how we would react to a foreign country's 'search' of our defense-related computer systems based upon a warrant from that country's courts."[65] A U.S. search warrant will be of little use when a different country does not wish to cooperate.[66] If law enforcement agencies need to get warrants from all other courts to begin an investigation, enforcing laws against fraud is that much more difficult.

One can dream up a world where all the laws and legal procedures were the same, but such circumstances are quite different than those in the world today. The President's Working Group explains the problem succinctly:

> The solution to the problems stemming from inadequate laws is simple to state, but not as easy to implement: countries need to reach a consensus as to which computer and technology-related activities should be criminalized, and then commit to taking appropriate domestic actions. Unfortunately, a true international 'consensus' concerning the activities that universally should be criminalized is likely to take time to develop. Even after a consensus is reached, individual countries that lack appropriate legislation will each have to pass new laws, an often time-consuming and iterative process.[67]

Although it may be possible for all countries to coordinate their laws and legal procedures, the likelihood of this happening in the near future is low.

The second problem arising from international fraud is that the question of what agency has jurisdiction is ill-defined.[68] Even if the laws and legal procedures are the same, what government will investigate and deal

---

64 President's Working Group, *supra* note 40.

65 *Id.*

66 Rothchild states, "Unduly aggressive enforcement action by government agencies in the context of cross-border online fraud risks giving rise to this sort of conflict, with detrimental effects on the efficacy of cross-border enforcement actions." Adding, that "the result can be conflict between two sovereigns." Rothchild, *supra* note 15, at 923.

67 President's Working Group, *supra* note 40.

68 *Internet and Federal Courts: Issues and Obstacles: Oversight Hearing Before the Subcommittee on Courts and Intellectual Property of the House Comm. on the Judiciary*, 106th Cong. (2000) (Statement of D. Jean Veta, Deputy Associate Attorney General, Department of Justice), *available at* http://commdocs.house.gov/committees/judiciary/hju66042.000/hju66042_0.htm.

with the fraud is an open question.[69] A merchant might be located in one country, a fraudster might be located in another country, and their computers might be located in yet another country. When fraud occurs, which government has jurisdiction? One might assume that a US company can simply turn to his local authorities, who coordinate with state and federal agencies, who in turn coordinate with authorities in the other nation. Despite the apparent simplicity, the situation is much more complicated.

Some examples can illustrate this problem. I listened to one former Silicon Valley executive describe his situation when his company was the victim of fraud originating in another country. When he attempted to follow standard procedures and contact officials, he soon realized that government would be of little help. He said, "There was a jurisdictional dispute between the FBI office in San Jose and San Francisco over which of them had jurisdiction over Kazakhstan, and which could handle it. So there were some very serious sorts of problems."[70] In the end the government did nothing to rectify his situation, and his company sustained tremendous losses due to fraud. Although the law against fraud is on the books, whether the government can do anything about it is uncertain.[71]

The classical-liberal conception of law enforcement is that all parties need to be subject to a monopolist arbiter of law.[72] Yet the ability for anyone with an Internet connection to transact with numerous parties around the globe brings into question where there can be a monopolist enforcer of law. Unlike spatially-based interaction, electronic commerce enables parties to interact without knowledge of their counterpart's location.[73] As more people interact with those outside their jurisdiction, it creates problems for government's geographically-based system of law. Incidentally, most of the classical-liberal arguments against private law enforcement apply to the situation at hand. How can parties interact when they are not both subject

---

69 Karen Alboukrek, *Adapting to a New World of E-Commerce: The Need for Uniform Consumer Protection in the International Electronic Marketplace*, 35 GEO. WASH. INT'L L. REV. 425, 434 (2003). Edward Stringham, *Market Chosen Law*, 14:1 J. LIBERTARIAN STUD. 53 (1999).

70 Presentation, Independent Institute, San Francisco, CA (April 21, 2004).

71 Wible, *supra* note 20, at 1581 (concluding that "With jurisdictional uncertainties looming in cases that are expensive to investigate and that require sophisticated tracking capabilities, state prosecution is almost impossible").

72 Gordon Tullock (ed.) Explorations in the Theory of Anarchy, (Center for the Study of Public Choice) (1972); Tyler Cowen, *Law as a Public Good: The Economics of Anarchy*, 8 ECONOMICS AND PHILOSOPHY 249 (1992); ROBERT NOZICK, ANARCHY, STATE, AND UTOPIA (1974).

73 The President's Working Group writes, "In the physical world, one cannot visit a place without some sense of its geographic location. Whether a particular street address or an area of the world, human travel is spatially based. By contrast, because one can access a computer remotely without knowing where, in physical space, that computer is located, many people have come to think of the collection of worldwide computer linkages as 'cyberspace.'" President's Working Group, *supra* note 40.

to the same enforcer of law? One potential solution would be world government, but the desirability of that is questionable. Whereas North argues that we need government enforcement as trade moves outside small groups, he does not have a theory about how government enforcement can function as the groups become so big as to encompass people from many different nations.

One potential solution advocated by some lawyers is to give governments the authority to enforce laws on people outside their jurisdiction.[74] That would ensure that a merchant and a fraudster could be subject to a government regardless of the parties' locations. Johnson and Post point out a number of problems with this position.[75] Do we really want to give all governments on earth the authority to enforce laws on any citizen? Should American citizens be subject to Singaporean law enforcement if the Singaporean police are conducting an investigation or a prosecution?[76] If any government could subject residents of any other country to its procedures, the few legal protections against search and seizure might vanish, and the result could be a race to the bottom of legal rights.[77] Whether the citizens around the world would want to be subjected to all other countries' laws is unclear. That means that a government model of international law enforcement would require some type of coordination between countries, which is the final requirement.

Requirement IV: Effective partnerships with other nations to encourage them to enact laws that adequately address cybercrime and to provide assistance in cybercrime investigations.

Following Reno's sentiment, Deputy Assistant Attorney General Bruce Swartz states that international enforcement of law requires the "establishment of strong mechanisms for international cooperation, since computer-related crimes are often committed via transmissions routed through numerous countries."[78] For example, if a U.S. agency identifies a fraudster residing in a different country, the U.S. agency has to work with the authorities in the second country if it wishes to enforce the law. Even assuming that the laws are the same and the jurisdictional issues are sorted out,

---

74 Michael Geist, *Cyberlaw 2.0*, 44 B.C L. REV. 323 (2003), 345-7; Rothchild, *supra* note 15, at 986.

75 Johnson & Post, *supra* note 58.

76 To lawyers such as Geist, the answer is actually yes. Michael Geist, *Cyberlaw 2.0*, 44 B.C. L. Rev. 323, 345-47 (2003).

77 Laura W. Murphy, *ACLU Letter to the Senate Foreign Relations Committee on the Council of Europe Convention on Cybercrime*, (ACLU), June 16, 2004.

78 Multilateral Law Enforcement Treaties, June 17, 2004 (See statement of Bruce Swartz, Deputy Assistant Attorney General, Criminal Divison, Senate Foreign Relations Committee).

the extent to which different countries can coordinate their efforts is unclear.

One can imagine a world where all law enforcement agencies work in concert at little cost, but clearly the world is quite different. Given that even intranational coordination between agencies is often difficult, international coordination will likely remain more difficult. Contacting other law enforcement agencies and getting them involved in a case is usually time consuming and costly. The President's Working Group explains the problem: "law enforcement agencies are burdened with cumbersome mechanisms for international cooperation, mechanisms that often derail or slow investigations."[79] If an investigation is time sensitive, delays between agencies can stifle a would-be investigation.[80] Unless the U.S. government can rely on governments around the globe to assist and enforce its laws, then people will be able to commit fraud in other countries and remain outside the law.[81] Yet prohibition of fraud hinges on the law being enforced regardless of where the fraudster resides. The President's Working Group recognizes this very real problem: "With scores of Internet-connected countries around the world, the coordination challenges facing law enforcement are tremendous."[82] The result is that even though international fraud might attract attention from multiple law enforcement agencies, it possibly might attract the attention of none.[83]

The only real way to solve the problem would be to have tremendous coordination between law enforcement agencies around the globe. The President's Working Group brings up the many difficult requirements.

> Because the gathering of information in other jurisdictions and internationally will be crucial to investigating and prosecuting cybercrimes, all levels of government will need to develop concrete and reliable mechanisms for cooperating with each other. The very nature of the Internet—its potential for anonymity and its vast scope—may cause one law enforcement agency to investigate, inadvertently, the activities of another agency that is conducting an undercover operation. Likewise, the law enforcement agency of one state may require the assistance of another for capturing and extraditing a criminal to its state for prosecution. In other words, crimes that were once planned and executed in a single jurisdiction are now

---

79 President's Working Group, *supra* note 40.

80 *Id.*

81 Alboukrek, *supra* note 69, at 440.

82 President's Working Group, *supra* note 40.

83 Rothchild writes, "A technique commonly employed by professional perpetrators of consumer fraud is to set up operations in one country, but to target only residents of other countries. They hope that by doing so they will slip under the radar of law enforcement authorities, as authorities in the country in which they are located will perceive little interest in expending resources to protect foreign consumers, and authorities in the country where the victims are located will face practical difficulties in taking action against a seller located outside the country. In some cases, the laws are inadequate to respond to this problem. n110" Rothchild, *supra* note 15, at 921.

> planned in one jurisdiction and executed in another, with victims throughout the United States and the world. [84]

As wrongs can be planned and committed across borders, government enforcement would require the law enforcement in all countries to coordinate. The government would either need bilateral agreements with every country or a multilateral agreement with all countries. The Council of Europe has spent the past fifteen years debating and drafting a Cybercrime Convention, which to date has yet to be ratified.[85] Perhaps not surprisingly, the Cybercrime Convention has little to do with protecting online merchants and more to do with regulating business and creating laws against hate speech. International politics does not operate in a classical-liberal vacuum, so the treaty contains numerous aspects which are opposed by groups ranging from the US Chamber of Commerce to the American Civil Liberties Union.[86] Although matters may change, the likelihood of a worldwide multilateral agreement (or numerous bilateral agreements) to help online merchants does not seem high.[87]

Critics of private self-governance argue that without uniform government standards, competition will lead to a race to the bottom, where the weakest level of self-regulation will prevail.[88] One can debate the validity of this argument against self-regulation,[89] but it seems to apply to the current problem with multiple governments. If one country has lax laws or inferior enforcement ability, fraudsters can set up operations in that country knowing that the likelihood of getting caught is less. The President's Working Group writes, "Inadequate regimes for international legal assis-

---

84 President's Working Group, *supra* note 40.

85 UNITED STATES DEPARTMENT OF JUSTICE, FREQUENTLY ASKED QUESTIONS AND ANSWERS ABOUT THE COUNCIL OF EUROPE CONVENTION ON CYBERCRIME (2001); LAURA W. MURPHY, AM. CIVIL LIBERTIES UNION, ACLU LETTER TO THE SENATE FOREIGN RELATIONS COMM. ON THE COUNCIL OF EUROPE CONVENTION ON CYBERCRIME (2004).

86 Press Release, Linda S. Rozett, Media Relations Dir., U.S. Chamber of Commerce, U.S. Chamber Opposes European Cyber Crime Treaty (Dec. 8, 2000); LAURA W. MURPHY, AM. CIVIL LIBERTIES UNION, ACLU LETTER TO THE SENATE FOREIGN RELATIONS COMM. ON THE COUNCIL OF EUROPE CONVENTION ON CYBERCRIME (2004).

87 Even the people who believe that all countries have the same goals still do not put a lot of faith in governments ability to coordinate. Breslin writes, "These governments, international organizations, and businesses also agree on general policy issues concerning electronic commerce. For example, these institutions want to foster consumer trust and security, protect privacy, and permit continued technological innovation. When it comes time to act, however, general policy agreement does not necessarily translate into a consistent global regulatory scenario or perhaps even the likelihood of one in the future." Adrienne J. Breslin, Electronic Commerce: Will It Ever Truly Realize Its Global Potential? 20 PENN ST. INT'L L. REV. 275, 299 (2001).

88 Joel Trachtman, Regulatory Competition and Regulatory Jurisdiction, 3 J. INT'L ECON. L. 331 (2000).

89 Roberta Romano, Empowering Investors: A Market Approach to Securities Regulation, 107 YALE L.J. 2359 (1998).

tance and extradition can therefore, in effect, shield criminals from law enforcement: criminals can go unpunished in one country, while they thwart the efforts of other countries to protect their citizens."[90] Although classical liberals such as Richard Epstein argue that government is created to eliminate externalities,[91] unless all the externalities in the globe can be internalized, externalities between nations will still exist.

One of the classical-liberal arguments against private enforcement is that prohibitions against wrongdoing create spillover benefits to all people in society. Even if private parties could solve the problem, private parties would bear all the costs and not gain all of the benefits, so a free-rider problem would be present. Thus, according to the classical liberal, the government steps in to eliminate the externalities. But the arguments of why private law enforcement cannot function are just as easily applied to the current situation. Any effort by one country to prevent online fraud would be costly and would provide benefits to all other nations. The costs are local and the benefits are not, so the same free-rider problem may rear its ugly head. If the U.S. government devotes resources preventing wrongs in other countries, American taxpayers foot the bill and see little results. Public-goods theory notwithstanding, there is little evidence that law enforcement agencies act to maximize the social-welfare function of the entire world. Law enforcement agencies have objectives and limited budgets just like anyone else, so to assume that they only act to serve the global public good might be unrealistic.

Even if we assume that all law enforcement agencies act to reduce fraud, they may have different incentives to do so. For example, each agency will likely want to devote resources to solving fraud against its own citizens, because the agency will appear better to voters than if it spent its resources helping residents abroad. Even if the culprits reside in the agency's country, victims in other countries give law enforcement agencies no political support, so governments have less incentive to help them. Reno brings up this important problem:

> While we are working with our counterparts in other countries to develop an international response, we must recognize that not all countries are as concerned about computer threats as we are. Indeed, some countries have weak laws, or no laws, against computer crimes, creating a major obstacle to solving and to prosecuting computer crimes. I am quite concerned that one or more nations will become "safe havens" for cybercriminals.[92]

---

90 President's Working Group, *supra* note 40.

91 Richard Epstein, *Skepticism and Freedom: The Intellectual Foundations of Our Constitutional Order*, 6 U. PA. J. CONST. L. 657 (2004).

92 Janet Reno, Statement of Janet Reno Attorney General of the United States Before the United States Senate Committee on Appropriations, Subcommittee on Commerce, Justice, and State, "Cybercrime" (February 16, 2000) (transcript available at: http://www.cdt.org/security/dos/000216senate/reno.html).

Classical liberals must recognize that not all governments act according to public-goods theory. Even if governments had the ability to do so, it seems unlikely that all countries will take the same interest in going after cyber fraud. If we introduce the possibility that certain governments simply do not care about American merchants, the likelihood that foreign governments will devote resources to eliminating fraud becomes lower.[93] Given that numerous governments have little concern for business in general, it seems unrealistic to think that they will help prevent fraud against foreign businesses.

Problems are exacerbated by the fact that governments in other countries may be even less knowledgeable about computer technology than is U.S. law enforcement. Yet international coordination of law enforcement hinges upon law enforcement agencies in every nation being up to date in the latest technology. Assistant Attorney General Michael Chertoff said, "When we deal with a transborder cybercrime, we *need* foreign law enforcement counterparts who not only have the necessary technical expertise, but who are accessible and responsive, and who have the necessary legal authority to cooperate with us and assist us in our investigations and prosecutions" (emphasis added).[94] "Technical expertise," "accessible," and "responsive" are not words that usually come to mind when thinking of governments around the world. To expect law enforcement agencies in less developed countries to solve a problem that U.S. agencies are incapable of solving might be a bit questionable. Can anyone honestly expect the government of Zimbabwe to help enforce laws against online fraud?

3. CONCLUSION

One of the main justifications of government is the idea that markets require government prohibitions against fraud. Yet we must recognize that law enforcement is not a perfect agent that can enforce laws without cost. Even if problems exist, the government may not have the ability to solve them. Wishful thinking notwithstanding, in the current world few of the conditions that government needs to prohibit fraud are met. Government has been unable to keep up with technology, lacks the necessary resources, and has difficulties collecting evidence and locating perpetrators of fraud. Government also faces organizational and jurisdictional uncertainties be-

---

93 Rustad writes "It is difficult to discover the identity of cybercriminals, who often operate in countries with corrupt governments that encourage Internet crime as a developing industry. Crimes on the Internet cross national borders, creating the need for international cooperation in law enforcement." Rustad, *supra* note 31, at 86, 98-99.

94 *Fighting Cybercrime: Efforts by Federal Law Enforcement: Hearing Before the Subcomm. on Crime of the H. Comm. on the Judiciary*, 107th Cong. 106 (2001) (Statement of Michael Chertoff, Assistant Att'y Gen., Criminal Division, U.S. Department of Justice).

cause fraud can take place across national boundaries where laws and legal procedures differ. Effective prohibition against fraud would require coordination between all law enforcement agencies, a situation that appears unlikely. Under these conditions the ability for government to prohibit online fraud is extremely limited.

To date, governments do not appear close to solving the problem.[95] Describing all types of computer fraud, attorneys Kim, Pinter, and Witmeyer estimate that "no more than 10% of the crimes involving computers get reported to authorities; further, less than 2% result in convictions."[96] Private companies know they cannot rely on government to rectify the situation, so in many cases they avoid reporting incidents. Even if government had a 100-percent recovery rate, companies would be reluctant to involve law enforcement because the cost of the legal process may exceed the cost of the stolen goods.[97] As the probability of recovery approaches zero, it is no wonder why companies would not turn to the law. Attorney General John Ashcroft recognized this issue saying, "victims are often reluctant to refer their cases to law enforcement," and adding, "we hope to convince the high tech community that when they report incidents of cybercrime, they are not just doing the right thing for their community—they are also doing the right thing for their business."[98] To state the issue is to admit that government does little to help merchants victimized by fraud. If involving government was really in the interest of firms, they would not need persuasion from officials.

Although the evidence presented in this paper does not prove that law enforcement agencies are inherently incapable of prohibiting online fraud, it does show that they have been ineffective to date. The classical liberal might respond that all law enforcement needs is more resources and more laws.[99] The important fact remains that merchants have been unable to rely on prohibitions against fraud for virtually the entire history of electronic commerce. If past performance is any indicator of future success, we should not expect government to have the ability to solve the problem any-

---

95 Wible writes, "The first cases of computer crime were heralded as an unprecedented phenomenon that law was not equipped to handle. Scholars and policymakers have since proposed a number of deterrence strategies, from criminal sanctions to tort law and the architecture of the web itself, but none of these methods has proved successful." Wible, *supra* note 21, at 1581.

96 Alex Kim, Edward Pinter, and John Witmeyer, *Fraud Over the Internet: The Same Old Story, Different Medium*, E-Zine of Ford Marrin Esposito & Gleser, LLP, January 2000, http://www.fmew.com/archive/fraud/index.html.

97 Albert, *supra* note 1, at 588.

98 John Ashcroft, U.S. Attorney Gen., Attorney General Ashcroft's Speech Announcing Expansion of CHIP Program and Establishment of Nine New CHIP units (July 20, 2001) (U.S. Department of Justice's transcript *available at* http://www.usdoj.gov/criminal/cybercrime/chipagsp.htm).

99 President's Working Group, *supra* note 40.

time soon. As Janet Reno stated, "these challenges are daunting."[100] Another, perhaps more realistic, way of looking at the problem is to recognize that government is not close to being able to solve the problem.

The situation and the proposed government solution are not as simple as the classical liberals assume. After looking at the evidence, we come to the exact opposite conclusion as Douglas North. In contrast to North, who argued that government must provide external enforcement as markets move outside of small circles, we have found that government enforcement becomes less possible in these circumstances. Relatively anonymous markets such as electronic commerce may pose problems for trade, but they pose even more problems that perplex government. Just because a problem exists does not mean that government has the ability to provide the solution. Whether the market breaks down as classical-liberal theory would assume is left to future research. Preliminary observation, however, suggests that electronic commerce is alive and well despite the fact that merchants are unable to rely on the law. This seems to indicate that markets are more robust than classical liberals assume. Indeed, Klein, Benson, Rothbard, Friedman, Caplan, and Stringham argue precisely that.[101]

One of the great contributions of economists is to point out that public policy requires more than wishful thinking.[102] Coming up with a theory of how markets are imperfect and how government can solve the problem is not enough. But lawyers and economists such as Epstein and North are guilty of exactly this. Classical liberals have theorized how markets require government prohibitions against fraud and how government can solve the problem. Yet in reality, the situation is quite different. George Mason economist Alex Tabarrok warns against what he calls theoretical empiricism.[103] People come up with a theory and then assume that the world conforms to their theory. But just because one assumes that the government can solve the problem does not mean that it actually can. It seems that classical liberals are indeed guilty of the Nirvana fallacy.

---

100 Janet Reno, Statement of Janet Reno Attorney General of the United State Before the United States Senate Committee on Appropriations, Subcommittee on Commerce, Justice, and State, "Cybercrime," February 16, 2000.

101 BRUCE L. BENSON, THE ENTERPRISE OF LAW: JUSTICE WITHOUT THE STATE (1990); MURRAY N. ROTHBARD, FOR A NEW LIBERTY: THE LIBERTARIAN MANIFESTO (Fox and Wilkes 1989) (1973); DAVID D. FRIEDMAN, THE MACHINERY OF FREEDOM: GUIDE TO RADICAL CAPITALISM (2d. ed. Open Court 1989) (1971); Bryan Caplan and Edward Stringham, *Networks, Law, and the Paradox of Cooperation*, 16 REV. OF AUSTRIAN ECON. 309 (2003).

102 Harold Demsetz, *Information and Efficiency: Another Viewpoint*, 12 J.L. & ECON. 1 (1969); LUDWIG VON MISES, ECONOMIC CALCULATION IN THE SOCIALIST COMMONWEALTH (S. Adler trans., Ludwig von Mises Institute, 1990) (1920); George J. Stigler, *Public Regulation of the Securities Markets*, 37 J. OF BUS. 117 (1964).

103 Alex Taborrok, *Market Challenges and Government Failure: Lessons from the Voluntary City*, In the Voluntary City: Choice, Community, and Civil Society 405-28 (David T. Beito, et al. eds., University of Michigan Press 2002).